UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,274	02/16/2004	Giovanni M. Della-Libera	MS1-1858US	2211

22801 7590 08/18/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
08/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/780,274	DELLA-LIBERA ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-8,10-36 and 38-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-8,10-36 and 38-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the Request for Continued Examination filing of 06/17/2008. Claims 1-4, 6-8, 10-36, and 38-48 are pending and have been considered as follows.

Specification

1. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

- Claims 1 & 38 lines 4-6 recite "a first format" and "a second format" and "the first format" however, the applicant's Specification does not appear to provide antecedent basis for these limitations;

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1 and 38 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not

described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

- Claims 1 & 38 lines 4-6 recite "a first format" and "a second format" and "the first format" however, the applicant's Specification does not appear to provide support for these limitations and are considered as new matter;

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 3, 4, 12, 13, 18, 20-23, 30, 31, 36, 38-40, 43, & 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen (US-5638448-A).

Claim 1:

Nguyen discloses a method of processing multiple types of security schemes comprising,

- "receiving a message having a first token and a second token" (i.e. "The 64 bit value R is used as a DES key to encrypt the user ID. This makes the user ID look random for each logon packet…The client generates a key Ka from the user ID and password using a one way hash function such as the Secure Hash Standard (SHS) specified in the Federal

Information Processing Standards Publication 180 (FIPS PUB 180)…When the server receives the first logon packet it decrypts the packet as follows") [column 4 lines 8-10, 13-17, & 22-23];

- "wherein the first token is in a first format and the second token is in a second format that is different from the first format, associated with a same subject" (i.e. "The 64 bit value R is used as a DES key to encrypt the user ID. This makes the user ID look random for each logon packet…The client generates a key Ka from the user ID and password using a one way hash function such as the Secure Hash Standard (SHS) specified in the Federal Information Processing Standards Publication 180 (FIPS PUB 180)") [column 4 lines 8-10, 13-17];
- "authenticating the first token by extracting a first claim from the first token" (i.e. "If the user is authorized, the server uses the decrypted 64 bit value R in the packet header as a key to decrypt the user ID") [column 4 lines 31-35];
- "authenticating the second token by extracting a second claim from the second token" (i.e. "If access date and time are verified, the server retrieves an associated one way hashed password Kb from an encrypted password file to decrypt the random number Ra and the CRC signatures. The password file is encrypted with a key Kk which is selected by the system administrator at installation") [column 4 lines 40-47];
- "wherein the first and second claims comprise different statements about the subject" (i.e. "The 64 bit value R is used as a DES key to encrypt the user ID. This makes the user ID look random for each logon packet…The client generates a key Ka from the user ID and password using a one way hash function such as the Secure Hash Standard (SHS)

specified in the Federal Information Processing Standards Publication 180 (FIPS PUB 180)…When the server receives the first logon packet it decrypts the packet as follows") [column 4 lines 8-10, 13-17, & 22-23];

- "authorizing access to a resource referred to in the message based at least in part on the first and second claims" (i.e. "The server manipulates the random number Rb with the same predefined formula used by the client and verifies if the random numbers are matched. If the random numbers match, then the server knows it is communicating with an authorized client and that the first logon packet was not a replayed packet") [column 5 lines 17-22];

but, Nguyen does not explicitly disclose,

- "grouping the first and second claims into a claim collection by selectively mapping the first claim and the second claim to other claims," although Nguyen does suggest information affiliated with the user attempting access determining the kind of access the user is permitted, as recited below;

however, Nguyen does disclose,

- "The ACLs are managed by network administrators to define to which resources a user can access and what kind of accesses the user has to each resource" [column 11 lines 50-53];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "grouping the first and second claims into a claim collection by selectively mapping the first claim and the second claim to other claims," in the invention as disclosed by Nguyen for the purposes of assigning access permissions based on the specific user ID where each users' password has a direct correlation with each user ID.

Claim 20:

Nguyen discloses a method of processing multiple types of security schemes comprising,

- "one or more computer processors" (i.e. "processor") [column 1 line 24];
- "one or more computer readable storage media" (i.e. "data storage") [column 1 lines 24-25];
- "executable by the one or more computer processors, to store: a first module to extract a first claim from a first token and a second claim from a second token associated with a message" (i.e. "If the user is authorized, the server uses the decrypted 64 bit value R in the packet header as a key to decrypt the user ID…If access date and time are verified, the server retrieves an associated one way hashed password Kb from an encrypted password file to decrypt the random number Ra and the CRC signatures. The password file is encrypted with a key Kk which is selected by the system administrator at installation") [column 4 lines 31-35 & 40-47];
- "wherein the message has an associated subject" (i.e. "the user") [column 4 line 9];
- "the first claim and the second claim comprise different statements related to the subject" (i.e. "The 64 bit value R is used as a DES key to encrypt the user ID. This makes the user ID look random for each logon packet…The client generates a key Ka from the user ID

and password using a one way hash function such as the Secure Hash Standard (SHS) specified in the Federal Information Processing Standards Publication 180 (FIPS PUB 180)…When the server receives the first logon packet it decrypts the packet as follows") [column 4 lines 8-10, 13-17, & 22-23];

but, Nguyen does not explicitly disclose,

- "a second module to selectively map the first claim and the second claim to other claims," although Nguyen does suggest information affiliated with the user attempting access determining the kind of access the user is permitted, as recited below;

however, Nguyen does disclose,

- "The ACLs are managed by network administrators to define to which resources a user can access and what kind of accesses the user has to each resource" [column 11 lines 50-53];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a second module to selectively map the first claim and the second claim to other claims," in the invention as disclosed by Nguyen for the purposes of assigning access permissions based on the specific user ID where each users' password has a direct correlation with each user ID.

Claim 38:

Nguyen discloses a method of processing multiple types of security schemes comprising,

- "receiving a message having a first token and a second token" (i.e. "The 64 bit value R is used as a DES key to encrypt the user ID. This makes the user ID look random for each logon packet…The client generates a key Ka from the user ID and password using a one

way hash function such as the Secure Hash Standard (SHS) specified in the Federal Information Processing Standards Publication 180 (FIPS PUB 180)…When the server receives the first logon packet it decrypts the packet as follows") [column 4 lines 8-10, 13-17, & 22-23];

- "wherein the first token is in a first format and the second token is in a second format that is different from the first format, associated with a same subject" (i.e. "The 64 bit value R is used as a DES key to encrypt the user ID. This makes the user ID look random for each logon packet…The client generates a key Ka from the user ID and password using a one way hash function such as the Secure Hash Standard (SHS) specified in the Federal Information Processing Standards Publication 180 (FIPS PUB 180)") [column 4 lines 8-10, 13-17];
- "obtaining a first claim from the first token and a second claim from the second token" (i.e. "If the user is authorized, the server uses the decrypted 64 bit value R in the packet header as a key to decrypt the user ID…If access date and time are verified, the server retrieves an associated one way hashed password Kb from an encrypted password file to decrypt the random number Ra and the CRC signatures. The password file is encrypted with a key Kk which is selected by the system administrator at installation") [column 4 lines 31-35 & 40-47];
- "wherein the first and second claims comprise different statements about the subject" (i.e. "The 64 bit value R is used as a DES key to encrypt the user ID. This makes the user ID look random for each logon packet…The client generates a key Ka from the user ID and password using a one way hash function such as the Secure Hash Standard (SHS)

specified in the Federal Information Processing Standards Publication 180 (FIPS PUB 180)…When the server receives the first logon packet it decrypts the packet as follows") [column 4 lines 8-10, 13-17, & 22-23];

but, Nguyen does not explicitly disclose,

- "selectively mapping the first claim and the second claim to other claims," although Nguyen does suggest information affiliated with the user attempting access determining the kind of access the user is permitted, as recited below;

however, Nguyen does disclose,

- "The ACLs are managed by network administrators to define to which resources a user can access and what kind of accesses the user has to each resource" [column 11 lines 50-53];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "selectively mapping the first claim and the second claim to other claims," in the invention as disclosed by Nguyen for the purposes of assigning access permissions based on the specific user ID where each users' password has a direct correlation with each user ID.

Claims 3, 21, & 39:

Nguyen discloses a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 1, 20, & 38 above, further comprising,

- "rejecting the message as a function of the first claim" (i.e. "If the access record cannot be found, the user has entered an invalid ID and the session is terminated") [column 4 lines 35-37].

Claims 4, 22, & 40:

Nguyen discloses a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 1, 20, & 38 above, further comprising,

- "rejecting the message as a function of the second claim" (i.e. "The server calculates the CRC signature of the packet header, the user ID and the random number Ra. If the calculated signatures match the decrypted signatures C1 and C2 stored in the packet, and if password Ka matches Kb, the server manipulates the client random number Ra with a predefined formula, generates a random number Rb, and encrypts both random numbers Ra and Rb with the password Kb before sending the first logon response packet to the client") [column 4 lines 48-55].

Claims 12, 30, & 43:

Nguyen discloses a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 1, 20, & 38 above, further comprising,

- "sending a return message to a sender of the message" (i.e. "sending the first logon response packet to the client") [column 4 lines 54-55];

- "the return message includes information regarding the second claim" (i.e. "If access date and time are verified, the server retrieves an associated one way hashed password Kb from an encrypted password file to decrypt the random number Ra and the CRC signatures… if password Ka matches Kb, the server manipulates the client random number Ra with a predefined formula, generates a random number Rb, and encrypts both random numbers Ra and Rb with the password Kb before sending the first logon response packet to the client") [column 4 lines 40-43 & 50-55].

Claims 13 & 31:

Nguyen disclose a method of/a system configured to processing multiple types of security schemes, as in Claims 12 & 30 above, further comprising,

- "the information regarding the second claim comprises the second claim" (i.e. "The client generates a key Ka from the user ID and password using a one way hash function such as the Secure Hash Standard (SHS) specified in the Federal Information Processing Standards Publication 180 (FIPS PUB 180)") [column 4 lines 12-16].

Claims 18, 36, & 48:

Nguyen discloses a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 1, 20, & 38 above, further comprising,

- "sending the message, the first token and the second token to another entity" (i.e. "The second step in the process takes place at the server. When the server receives the first logon packet it decrypts the packet as follows") [column 4 lines 21-23];

- "the second token includes information related to the second claim" (i.e. "The client generates a key Ka from the user ID and password using a one way hash function such as the Secure Hash Standard (SHS) specified in the Federal Information Processing Standards Publication 180 (FIPS PUB 180)") [column 4 lines 12-16].

Claim 23:

Nguyen discloses a system configured to process multiple types of security schemes, as in Claim 20 above, further comprising,

- "a module to form a claim collection that includes the first and second claims" (i.e. "The ACLs are managed by network administrators to define to which resources a user can access and what kind of accesses the user has to each resource") [column 11 lines 50-53].

6. Claims 2, 6, 8, 10, 11, 14-17, 24, 26-29, 32-35, 41, 42, & 44-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen (US-5638448-A) in view of Benantar et al. (US-6854056-B1).

Claim 2:

Nguyen discloses a method of processing multiple types of security schemes, as in Claim 1 above, but Nguyen does not explicitly disclose,

- "obtaining another claim from the token," although Benantar et al. do suggest digital certificates, as recited below;

however, Benantar et al. do disclose,

- "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems" [column 7 lines 61-65];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining another claim from the token," in the invention as disclosed by Nguyen for the purposes of providing additional information for verifying a user's identity through the usage of digital certificates.

Claims 6, 24, & 41:

Nguyen discloses a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 1, 20, & 38 above, but Nguyen does not explicitly disclose,

- "obtaining a resource identifier from the message," although Benantar et al. do suggest identity information and an associated secret, as recited below;

however, Benantar et al. do disclose,

- [Fig 8c illustrates obtaining host identities and associated secret];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a resource identifier from the message," in the invention as disclosed by Nguyen for the purposes of providing additional information for verifying a user.

Claims 8 & 26:

Nguyen and Benantar et al. disclose a method of/a system configured to processing multiple types of security schemes, as in Claims 6 & 24 above, but Nguyen does not explicitly disclose,

- "the resource identifier comprises a property of the message," although Benantar et al. do suggest host identity information and an associated secret, as recited below;

however, Benantar et al. do disclose,

- [Fig 8c illustrates host identity associated secret];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the resource identifier comprises a property of the message," in the invention as disclosed by Nguyen for the purposes of providing additional information for verifying a user.

Claim 27:

Nguyen discloses a system configured to processing multiple types of security schemes, as in Claim 20 above, but Nguyen does not explicitly disclose,

- "a module to selectively obtain a resource identifier from a computing system in which the first and second modules reside," although Benantar et al. do suggest obtaining host identities and associated secret(s), as recited below;

however, Benantar et al. do disclose,

- [Fig 8c illustrates obtaining host identities and associated secret];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a module to selectively obtain a resource identifier from a computing system in which the first and second modules reside," in the invention as disclosed by Nguyen for the purposes of providing additional information for verifying a user.

Claims 10 & 28:

Nguyen and Benantar et al. disclose a method of/a system configured to processing multiple types of security schemes, as in Claims 6 & 27 above, but Nguyen does not explicitly disclose,

- "the resource identifier comprises a property of the computing system's runtime environment," although Benantar et al. do suggest host identity and associated secret, as recited below;

however, Benantar et al. do disclose,

- [Fig 8c illustrates host identity associated secret];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the resource identifier comprises a property of the computing system's runtime environment," in the invention as disclosed by Nguyen for the purposes of providing additional information for verifying a user.

Claims 11, 29, & 42:

Nguyen and Benantar et al. disclose a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 6, 27, & 38 above, but Nguyen does not explicitly disclose,

- "a resource corresponding to the resource identifier is stored by the computing system," although Benantar et al. do suggest authentication taking place at an external system, as recited below;

however, Benantar et al. do disclose,

- [Fig 8c illustrates a client being authenticated to additional outside systems];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a resource corresponding to the resource identifier is stored by the computing system," in the invention as disclosed by Nguyen for the purposes of providing an external system for performing authentication using multiple elements of identification for the purposes of user verification.

Claims 14, 32, & 44:

Nguyen discloses a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 1, 20, & 38 above, but Nguyen does not explicitly disclose,

- "rejecting the message as a function of the third claim," although Benantar et al. do suggest utilizing digital certificates, as recited below;

however, Benantar et al. do disclose,

- "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems" [column 7 lines 61-65];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "rejecting the message as a function of the third claim," in the invention as disclosed by Nguyen for the purposes of providing additional information that can verify a user's identity.

Claim 45:

Nguyen discloses a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claim 44 above, but Nguyen does not explicitly disclose,

- "obtaining a third claim from the first claim," although Benantar et al. do suggest utilizing digital certificates including additional information, as recited below;

however, Benantar et al. do disclose,

- [Fig 8c illustrates an authentication of a client based on host identity information and secret information];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a third claim from the first claim," in the invention as disclosed by Nguyen for the purposes of providing additionally identifiable information for the authentication and verification of a user.

Claims 15, 33, & 46:

Nguyen discloses a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 1, 20, & 38 above, but Nguyen does not explicitly disclose,

- "obtaining a third claim from the second claim," although Benantar et al. do suggest utilizing digital certificates, as recited below;

however, Benantar et al. do disclose,

- "a single digital certificate may contain many host identities, which may be found within the digital certificate by searching through the host names, thereby allowing the digital certificate to support host identity mapping on multiple host systems" [column 7 lines 61-65];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining a third claim from the second claim," in the invention as disclosed by Nguyen for the purposes of providing additional information that can verify a user's identity.

Claims 16, 34, & 47:

Nguyen discloses a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 1, 20, & 38 above, but Nguyen does not explicitly disclose,

- "selectively rejecting the first claim," although Benantar et al. do suggest utilizing digital certificates including additional information, as recited below;

however, Benantar et al. do disclose,

- [Fig 8c illustrates authentication of a client based on host identity information and secret information];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "selectively rejecting the first claim," in the invention as disclosed by Nguyen for the purposes of providing additionally identifiable information for the authentication and verification of a user.

Claims 17 & 35:

Nguyen discloses a method of/a system configured to processing multiple types of security schemes and a computer-readable storage medium storing computer-executable instructions that, when executed by a processor, as in Claims 1 & 20 above, but Nguyen does not explicitly disclose,

- "the token is received out-of-band from the message," although Benantar et al. do suggest permitting access after a user having an assigned identity has been identified, as recited below;

however, Benantar et al. do disclose,

- "The user may then access all applications or systems in which the user has an assigned identity within the distributed data processing system" [column 10 lines 48-51];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the token is received out-of-band from the message," in the invention as disclosed by Nguyen for the purposes of providing multiple pieces of information for the authentication and verification of a user.

7. Claims 7 & 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen (US-5638448-A) in view of Benantar et al. (US-6854056-B1) and in further view of Clark et al. ("XML Path Language").

Claims 7 & 25:

Nguyen and Benantar et al. disclose a method of/a system configured to processing multiple types of security schemes, as in Claims 6 & 24 above, but their combination do not explicitly disclose,

- "obtaining the resource from the message comprises applying an XPath expression," although Clark et al. do suggest utilizing XPath expressions, as recited below;
- "the module to obtain the resource identifier from the message is to selectively apply an XPath expression to obtain the resource identifier," although Clark et al. do suggest utilizing XPath expressions, as recited below;

however, Clark et al. do disclose,

- "XPath uses a compact, non-XML syntax to facilitate use of XPath within URIs and XML attribute values" [page 3];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obtaining the resource from the message comprises applying an XPath expression" and "the module to obtain the resource identifier from the message is to selectively apply an XPath expression to obtain the resource identifier," in the invention as disclosed by Nguyen and Benantar et al. for the purposes of .

Response to Arguments

8. Applicant's arguments with respect to Claims 1-4, 6-8, 10-36, and 38-48 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendments.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Butt et al. (US-6754829-B1) - certificate-based authentication system for heterogeneous environments;

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OAL/
08/14/2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136